Software Product Description

PRODUCT NAME: AltaVista Firewall 98 **SPD 64.21.05**

DESCRIPTION

AltaVista Firewall provides a secure and flexible connection between a trusted private network and an insecure public network, such as the Internet. It may also be used to secure portions of the private network within an organization. It protects the private network from unauthorized access, while providing controlled access to Internet services to users within the private network.

AltaVista Firewall combines trusted application proxies for controlling access with utilities for strong user authentication, comprehensive logging, reporting, and real-time alarms. It provides a comprehensive graphical user interface (GUI) to ease firewall configuration and management. It also provides secure remote management via an encrypted network connection, allowing a remote client to monitor, control, and configure the firewall.

AltaVista Firewall provides trusted application proxies that allow users access to most common services on the Internet, including Web, file transfer (FTP), remote terminal sessions (TELNET), electronic mail (SMTP), RealPlayer, SQL*Net and Finger. It also includes user-configurable generic TCP and UDP proxies. The application proxies enforce robust security checks to protect against unauthorized access. The proxies can be configured to allow controlled access from the internal network to the public network, and also from the public network into the internal network.

AltaVista Firewall provides a selection of predefined security policies appropriate to each application proxy. These security policies can be set up via the GUI. In addition, customized security policies can be developed via the GUI for all of the application proxies. Security policies can be configured to restrict access to specified groups of users and servers, as well as on the basis of time.

User authentication is available for Web, FTP, and TELNET access to and from the internal network. This allows access to be restricted to individual users. A variety of authentication methods are provided, including handheld authentication cards, once-off passwords, and reusable passwords. Handheld authentication cards are not included with the AltaVista Firewall product and must be purchased separately.

AltaVista Firewall performs comprehensive logging of all events relating to the operation of the firewall. A wide range of summary and detailed reports can be generated from the information in the log files.

AltaVista Firewall supports automatic, real-time alarms to alert the system manager of unusual or potentially threatening events on the firewall. The alarm system monitors the system log files for suspicious events, and triggers one or more alarm actions in response.

AltaVista Firewall runs on a dedicated hardware system. To maximize the security of the firewall, DIGITAL recommends that there are no user accounts on the system on which AltaVista Firewall is installed, and that no other applications run on the system. The system should also be secure from physical intrusion.

AltaVista Firewall can be set up as a "firewall-within-a-firewall" (i.e., an Intranet firewall), where an organization requires a portion of its private network to be secured using an internal firewall. This allows the secure portion of the private network to have secure connectivity to the remaining portion of the private network, and also connectivity to the external network via a second firewall. AltaVista Firewall also works with AltaVista Tunnel to provide a truly secure Virtual Private Network (VPN) environment.

AltaVista Firewall is based on technology that has been tried and tested in DIGITAL's own network for over a decade.

APPLICATION PROXIES

The firewall uses application proxies to provide users on the internal network with secure connectivity to the public network. Robust security checking protects the internal network against unauthorized access from the public network, and can also be configured to prevent access to the public network from the internal network, if required.

The firewall also controls the times at which each application proxy is available. You can configure each proxy to be available all the time; or only during specified business hours; or only outside specified business hours; or at specific times on named days. Application proxies are provided for the following services:

- World Wide Web (Web)

The Web application proxy can be used in both non-transparent mode and transparent mode (for outbound connections only). The Web proxy includes support for Secure Sockets Library (SSL) and can be configured to support data caching to improve response for heavily accessed Web sites. The proxy also includes support for HTTP, gopher, WAIS, FTP, HTTPS, and SNEWS URLs. The Web proxy uses the FTP application proxy to process FTP URLs, so that the security policy for FTP cannot be circumvented.

- Electronic Mail (SMTP)

The electronic mail proxy acts as a mail relay for SMTP mail between the external and internal networks. Incoming mail for the domain protected by the firewall is forwarded to a mail hub within the internal network for delivery. The mail proxy inspects the SMTP commands and message envelope to prevent attempts to subvert the firewall or the internal network.

- File Transfer (FTP)

The FTP application proxy can be used in both non-transparent mode and transparent mode (for outbound connections only). It provides support for both command line and windows-based FTP clients. The FTP proxy can be configured to control the FTP operations that can be performed, and hence the direction of data transfer. For example, the application proxy can control the ability of users to pull (GET) files or to push (PUT) files. Access can also be limited to users who are authenticated.

- Remote Terminal Service (TELNET)

The TELNET application proxy can be used in both non-transparent mode and transparent mode (for outbound connections only). The proxy includes support for TN3270 emulation. Access can also be limited to users who are authenticated.

- Finger

The finger application proxy prevents users on the public network from accessing the internal network using the finger command.

- SQL*Net

This SQL*Net proxy enables users to access data repositories across the Internet. SQL*Net establishes a connection to a database when a client or another database server process requests a database session.

NOTE: the SQL*Net proxy does not run on Alpha processors running Windows NT.

- RealPlayer

RealPlayer is an application that allows playback of audio and video in real-time over Internet connections. Through the RealPlayer application proxy, system administrators can decide whether users on internal network system can access RealPlayer services on the external network.

- Generic TCP

The firewall also provides a customizable generic TCP application proxy, which provides secure TCP connections to services that do not use a dedicated application proxy. The generic TCP proxy enables the firewall administrator to set up secure connections from one or many hosts to one destination host, with each connection limited to a single service.

- Generic UDP

A customizable generic UDP proxy allows UDP based applications, such as Internet Chat, to pass securely through the AltaVista Firewall.

- Pre-Configured Generic

AltaVista Firewall also delivers pre-configured generic proxies for protocols such as News (NNTP).

SECURITY POLICIES

AltaVista Firewall can block URLs to preserve network performance and to restrict access to specific Web sites. Administrators can define specific policies for URL access.

AltaVista Firewall can detect and block Java applets entirely by allowing selective filtering of Java applets through the firewall. Finjan's Java screening software can be integrated with AltaVista Firewall for Windows NT (Intel) to minimize the possibility that "bad" Java applets are allowed onto the intranet.

All of the application proxies support custom security policies defined by the firewall administrator. A custom policy is defined by a set of rules. Each rule contains the following elements:

- A group of named users to whom the rule applies. You can also specify the hosts from which the users connect.
- A group of named servers to which the users connect. You can also specify a port number for a service on the server.
- Whether the rule allows the users to use the service or denies them from using it.

- For the FTP proxy only, the sets of FTP commands to which the rule applies.

Groups of named users and groups of named servers can be created through the user interface. Sets of predefined security policies are provided for the Web, FTP, TELNET, and Finger proxies.

"IP Spoofing" Software

The firewall product incorporates dedicated software to prevent "IP spoofing" attacks. All packets that are received on the external network interface of the firewall but appear to originate from an address on the internal network are rejected.

Content Vectoring Protocol (CVP) Support

CVP support enables the integration of third-party value-added products with AltaVista Firewall. The most common use of CVP is for vectoring data to virus checking products, like Symantec's Norton AntiVirus for Firewalls.

Demilitarized Zone (DMZ) Support

AltaVista Firewall's DMZ support now provides administrators with greater flexibility when configuring their security implementations. It offers more than a simple trusted/untrusted implementation by offering three LAN connections: one for the Internet, one for public servers (such as Web servers), and one for the intranet. It also provides a simple GUI that enables administrators to set security policies on DMZ hosted servers.

USER AUTHENTICATION

The firewall supports user authentication, using a variety of methods. The following methods of user-based authentication are supported:

- AssureNet Pathways SecureNet Key (SNK)
- Bell Communications Research S/Key
- CRYPTOCard Access Control Tokens
- "Once-off" passwords
- Racal Watchword keys
- Reusable passwords (supported for outbound connections only)
- Security Dynamics SecurID authentication tokens
- Windows NT domain authentication (Windows NT firewall only)

The GUI provides an authentication user management system, with a step-by-step guide to configuring the authentication methods (that is, programming a handheld authentication card or setting a password). To use any of the authentication methods that require handheld cards, you must purchase the handheld cards separately. To use Security Dynamics SecurID cards, you must also purchase the ACE/Server server software separately. The server software for the other authentication methods is included in the AltaVista Firewall product.

LOGGING

All firewall components perform data logging when in operation. This ensures that comprehensive records of firewall usage are maintained in log files. The firewall log system automatically manages data logging and log file archiving. The firewall logging system monitors log file disk space and issues an alert if a predefined limit is exceeded. These features are user-configurable.

REPORTING

The firewall generates reports, which give a summary of the usage of the firewall and most individual services. Reports can be viewed via the GUI, mailed automatically at regular intervals to a specified list of users, or both. All reports use information from the system log files. A wide variety of summary and detailed reports are available.

SECURITY ALARMS

The sophisticated alarm and notification system continually monitors the firewall in real time and generates automatic alarms to alert the system administrator to unusual or potentially threatening events. Each alarm triggers one or more alarm actions, which include mailing or paging the administrator, raising the security status of the firewall, blacklisting the remote host from which the event was generated, and shutting down individual services or the whole firewall. AltaVista Firewall is installed with a default set of alarms, which are user-configurable.

The firewall uses a color-coded security status to indicate at a glance whether the firewall is under attack. Four security status levels are defined: green, yellow, orange, and red. The security status can be raised automatically by alarms, or changed manually by the system administrator.

GRAPHICAL USER INTERFACE

A comprehensive graphical user interface (GUI) allows the firewall administrator to perform all initial configuration, administration, and management tasks. The GUI is displayed in a window of the Web browser, and consists of multiple frames. Separate frames show the current status of the firewall, and the most recent events that triggered alarms.

A login and a timeout feature also protect the GUI. After a specified period, the GUI times out and requires the administrator to log in again. This reduces the risk of intrusion if the GUI is left unattended. The timeout period can be configured or the timeout can be switched off, as required.

The GUI supports multiple firewall administrators where each administrator has an associated set of privileges that control which GUI operations can be performed. In addition, the GUI supports defining different sets of privileges for a given administrator depending on whether they are logged in to the GUI locally or remotely.

The product includes extensive online help, including task-oriented help; context-sensitive help on all significant screens in the user interface, and reference help.

REMOTE MANAGEMENT

Remote management allows administrators to monitor, control, and configure an AltaVista Firewall system from a remote host. AltaVista Firewall establishes an encrypted network connection that delivers a high level of security for remote firewall management.

AltaVista Firewall includes the AltaVista Tunnel Server software for secure remote management. This software has been modified to allow only one tunnel to be established to the firewall at a time. AltaVista Firewall also includes the AltaVista Tunnel Client for Windows software and 2 licenses for use with the AltaVista Firewall remote management capabilities. The packaged AltaVista Tunnel software is limited to 40-bit RSA RC4 keys only.

The graphical interface for remote management is provided via a Web browser in the same way as the firewall console. This provides the user with full access to the same firewall management functions both locally and remotely.

DUAL DNS SERVER

AltaVista Firewall can be configured as a dual DNS server that understands which name services are internal or external. This dual DNS server is fully configurable through the GUI management.

HARDWARE REQUIREMENTS

Processors Supported:

- DIGITAL UNIX: Alpha processor capable of running a supported operating system version
- Windows NT: Intel or Alpha processor capable of running a supported operating system version

Other Hardware Required:

The system must include a monitor and be capable of running a supported Web browser version.

The system on which AltaVista Firewall is installed must also be capable of supporting two network interfaces. The type of network interface used depends on the network environment in which AltaVista Firewall is used. For example, if the system is connected to two local area networks over Ethernet, then two Ethernet connectors are required. If the firewall's external connection is through a dial-up connection, a supported modem card can be used in place of one of the network interfaces.

To install AltaVista Firewall, the system must support a CD-ROM reader.

Disk Space Requirements:

Operating System Platform	Installation	Use (Permanent)
DIGITAL UNIX	25 MB	1 GB
Windows NT	11 MB	2 GB

These counts refer to the disk space required on the system disk. The sizes are approximate; actual sizes may vary depending on the system environment, configuration, and software options.

AltaVista Firewall creates extensive log files as part of its normal operation. For this reason, a minimum of 1 or 2 GB of disk space is required to store log files. More space may be required, depending on the configuration of the individual site and the level of usage of AltaVista Firewall.

Memory Requirements:

- DIGITAL UNIX: 32 MB
- Windows NT: 48 MB

For optimum performance, 64 MB of memory is recommended.

SOFTWARE REQUIREMENTS

Operating System Requirements:

- DIGITAL UNIX Version 4.0B, 4.0C, or 4.0D
- Windows NT V4.0 (Service Pack 3 or higher)

Web Browser Support (for management):

- Microsoft Internet Explorer V3.0 or higher
- Netscape Navigator V3.0 or higher

DIGITAL UNIX Tailoring:

To use AltaVista Firewall for DIGITAL UNIX, you must install only the subsets of the operating system that are required by AltaVista Firewall. For specific information about these subsets and the operating system layout, refer to the AltaVista Firewall product documentation.

GROWTH CONSIDERATIONS

The minimum hardware/software requirements for any future version of this product may be different from the requirements for the current version.

DISTRIBUTION MEDIA

This product is available on CD-ROM.

ORDERING INFORMATION

For ordering Information, contact your AltaVista Business Partner or Digital Equipment Corporation.

SOFTWARE LICENSING

This software is furnished under the licensing provisions of Digital Equipment Corporation's Standard Terms and Conditions or the licensing terms accompanying the software. For more information about DIGITAL's licensing terms and policies, contact your local DIGITAL office.Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid license from DIGITAL or an authorized sublicensor.

SOFTWARE PRODUCT SERVICES

Standard remedial services as well as consulting services for planning, designing, and implementing a custom security system are available. For more information, contact your AltaVista Business Partner or your local DIGITAL office.

SOFTWARE WARRANTY

A limited warranty for this software product is provided by DIGITAL with the purchase of this software package. AltaVista Firewall 98 is considered Year 2000 Ready. For specific warranty details, please refer to http://www.digital.com/year2000.

This product is intended to assist customers in maintaining an appropriately secure systems environment when used in conjunction with customers' vigilant operational security practices. DIGITAL does not guarantee or warrant that the use of this product will provide complete security protection for customers' systems.

® Windows NT is a trademark of Microsoft Corporation.

® Netscape is a trademark of Netscape Communications Corporation.

® RealAudio, RealPlayer, and RealServer are trademarks of Progressive Networks, Inc.

® Intel is a registered trademark of Intel Corporation.

® Microsoft and Windows are registered trademarks of Microsoft Corporation.

® Security Dynamics, ACE/Server, and SecurID are registered trademarks of Security Dynamics Technologies, Inc.

® SQL*Net is a registered trademark of Oracle Corporation, Redwood City, California.

® UNIX is a registered trademark in the United States and other countries licensed exclusively through X /Open Company Ltd.

™ AlphaServer, AltaVista, DIGITAL, DIGITAL UNIX, and the DIGITAL logo are trademarks of Digital Equipment Corporation.

All other trademarks and registered trademarks are the property of their respective owners.